UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

March 22, 2024

Mr. Raymond V. Furstenau
Executive Director for Operations, Acting
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: FINAL DRAFT REVISION 9 OF STANDARD REVIEW PLAN BRANCH TECHNICAL POSITION 7-19, "GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON-CAUSE FAILURE DUE TO LATENT DEFECTS IN DIGITAL SAFETY SYSTEMS"

Dear Mr. Furstenau:

During the 713th meeting of the Advisory Committee on Reactor Safeguards, March 6-7, 2024, we completed our review of Final Draft Revision 9 of Standard Review Plan (SRP)(NUREG-0800), Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Defects in Digital Instrumentation and Control Systems." During this review, we had the benefit of discussions with representatives of the NRC staff during our Digital Instrumentation and Control (DI&C) Subcommittee meeting on February 22, 2024. We also had the benefit of the documents referenced.

CONCLUSIONS AND RECOMMENDATIONS

1. After incorporation of one clarification to Section B.3.4.4 as discussed below, the draft revision to BTP 7-19 will more completely reflect Commission Policy as promulgated in SRM-SECY-22-0076, and it can be issued.

2. The staff should develop a plan to complete an integrated staff guidance document for DI&C defense-in-depth and diversity assessments to maintain consistency across all reactor types.

3. Longer term suggestions to improve assessments of defense in depth and diversity are discussed below.

BACKGROUND

Digital technology offers significant operational and maintenance benefits for instrumentation and control systems in nuclear power plants (NPPs). DI&C systems are composed of both hardware components and logic elements (e.g., software). DI&C systems or components are vulnerable to common-cause failures (CCFs) similar to those considered for analog systems due to latent design defects in active hardware components, software, or software-based logic. A CCF occurs when multiple (usually identical) systems or components fail due to a shared

cause. CCFs can result in two different effects: (1) a loss of the capability to perform a safety function or initiate a plant transient, or (2) initiation of a function without a valid demand, resulting in erroneous system actions.

SRM-SECY-93-087 provided the Commission's policy on how potential CCFs should be addressed in DI&C systems considering the following four points:

1. Perform a defense-in-depth and diversity assessment to demonstrate CCF vulnerabilities were addressed,

2. Analyze each CCF for each event evaluated in the accident analysis section of the safety analysis report (SAR) using best estimate methods,

3. Provide a diverse means if the assessment shows a CCF could disable a safety function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions, and

4. Provide diverse displays and controls in the main control room for manual, system-level actuation of critical safety functions.

SECY-18-0090 clarifies the staff application of the Commission's direction within SRM-SECY-93-087. The BTP focusses the staff review guidance to satisfy Commission direction.

The BTP provides guidance for evaluating how defense in depth and diversity address vulnerabilities to CCF caused by latent defects in system hardware, software or software-based logic, as well as the effects of any unmitigated CCF outcomes on plant safety. Specifically, the BTP provides guidance for staff reviewing: (1) proposed design attributes, such as the use of diverse equipment, testing, or NRC-approved alternative methods, including defensive measures within the design of a system or component to eliminate the potential for CCF from further consideration, (2) diverse external equipment, including manual controls and displays to limit or mitigate a potential CCF, and (3) other measures to ensure conformance with the NRC's position on addressing potential CCFs in DI&C systems.

The guidance of the BTP is intended for staff reviews of DI&C safety systems with (1) proposed modifications that require implementation of a license amendment, and (2) applications for construction permits, operating licenses, combined licenses, design certifications, standard design approvals, and manufacturing licenses. The BTP is not applicable to proposed modifications performed under the change process in Title 10 of the *Code of Federal Regulations* (10 CFR) Section 50.59, "Changes, tests and experiments." Review criteria for single random failures and cascading failures from shared resources (i.e., not due to latent design defects in DI&C structures, systems and components) are not covered in the BTP.

On August 10, 2022, the staff submitted SECY-22-0076 to request that the Commission approve expanding the current policy regarding DI&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense in depth, including not providing any diverse automatic actuation of safety functions. This expanded policy would apply to requests for new or amended licenses and design approvals, for all NPP types, under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

On May 25, 2023, the Commission approved the SECY-22-0076 recommendation to expand the existing policy for DI&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense in depth, subject to their edits. Also, the Commission directed the staff to clarify in the implementing guidance that the new policy is independent of the licensing pathway selected by reactor licensees and applicants.

DISCUSSION

Approach to Incorporate the Commission Direction

The staff elected to take different approaches between light-water reactors (LWRs) and advanced non-LWRs.

For LWRs, which are covered by the SRP, staff made the following revisions to BTP 7-19 to incorporate risk-informed options:

- Within Section B.3, Detailed Defense-in-Depth and Diversity Assessment, added: 3.4 Risk-Informed Defense-in-Depth and Diversity Assessment, 3.4.1 Determining Consistency with NRC Policy and Guidance on Risk-Informed Decision-Making, 3.4.2 Modeling the CCF, 3.4.3 Determining the Risk Significance of the CCF, and 3.4.4 Determining the Appropriate Means to Address the CCF. Acceptance criteria were specified for each of the above sections.

- Within existing Section B.4, Manual System-Level Actuation and Indications, added revisions to address Commission direction that "*The applicant may alternatively propose a different approach to this point in the policy if the plant design has a commensurate level of safety.*" Acceptance criteria were also revised for consistency.

- Other revisions were made throughout the document for editorial and consistency purposes.

The LWR approach closely follows the policy described in SRM-SECY-22-0076. However, we are concerned that the text of the draft subsection B.3.4.4 is unclear and not consistent with the following statement in the SRM: "*If a postulated CCF is risk significant and the assessment does not demonstrate the adequacy of other design techniques, prevention measures, or mitigation measures, then a diverse means must be provided.*" This subsection should be revised to clearly direct an assessment of additional design/mitigation approaches or inclusion of diversity for cases where the CCF has been determined to be risk significant.

For non-LWRs, which were not addressed in this BTP revision, the staff elected to defer any revisions to guidance until more experience is obtained with use of the Design Review Guide (DRG), "Instrumentation and Controls for Non-LWR Reviews," dated February 26, 2021. While the language used in the DRG does not clearly connect to the revisions of the four points in SRM-SECY-22-0076, it does not preclude the reviewers from considering alternative approaches. Therefore, the staff intends to use pre-application engagement to discuss use of the expanded policy with interested applicants to address any questions or concerns. The staff plans to revise the DRG, and possibly Regulatory Guide (RG) 1.233, in the future based on lessons learned during upcoming interactions with stakeholders. The staff believes this experience is necessary to understand what guidance on these matters would be of use to non-LWR applicants.

The DRG incorporates guidance for assessing diversity in support of defense in depth that is much less detailed than the corresponding guidance in BTP 7-19. It is not clear that this less detailed level of guidance is sufficient for advanced non-LWRs. Thus, we have the following two suggestions for consideration by the staff:

- While the approach to defense in depth or risk-importance measures may be different between LWRs and non-LWRs, the detailed design of the DI&C systems will be very similar, with the same system designs likely used among multiple reactor technologies and similar approaches being taken to achieve diversity where needed. Use of a single guidance document would assist both applicants and NRC staff in development and review of DI&C system designs that are intended for application in multiple reactor technologies. Thus, we recommend the staff develop a plan for an integrated staff guidance document for DI&C defense in depth and diversity assessments that applies to all reactor types to maintain consistency between reactor designs. The plan should maintain alignment with development of appropriate risk importance measures for non-LWRs, considering that the RG 1.174 risk criteria (core damage frequency and large early release frequency) may not be applicable for the advanced/non-LWR reactors.

- The public comments provided on BTP 7-19 should be evaluated for non-LWRs. While it may be premature to make any changes to the DRG based on the public comments, they should be assessed to inform any preapplication discussions regarding DI&C system design. We suggest that the staff document their assessment of the applicability of the BTP 7-19 public comments to the DRG.

Characterization of Defense in Depth in BTP 7-19 and the DRG

Prior to Final Draft Revision 9, BTP 7-19 characterized DI&C system defense in depth using the DI&C system “echelons of defense” described in NUREG/CR-6303[1]. Final Draft Revision 9 eliminates discussion of these “echelons of defense” and also deletes specific reference to NUREG/CR-6303 from several of the detailed guidelines. Additionally, the DRG for advanced non-LWRs does not reference NUREG/CR-6303 nor does it discuss a framework using DI&C echelons in applying defense-in-depth. Use of DI&C echelons (derived from the applicable design-specific plant-capability defense-in-depth model) would help confirm the adequacy of DI&C system defense in depth when assessing vulnerability to CCFs. We recommend the staff ensure use of a logical echelon-type framework to address defense in depth in future DI&C applications.

SUMMARY

---

[1] NUREG/CR-6303 was issued in 1994 and defines four DI&C system “echelons of defense” that are derived from a plant defense-in-depth model which credits independent fuel cladding, reactor pressure vessel, and containment boundaries: (1) control system; (2) reactor trip system; (3) engineered safeguards features actuation system; and (4) monitoring and indication system. These four “echelons of defense” are the foundation for the diversity assessment methods described in the rest of NUREG/CR 6303.

After incorporation of one clarification to Section B.3.4.4 as discussed above, the Final Draft Revision to BTP 7-19 will more completely reflect Commission Policy as promulgated in SRM-SECY-22-0076, and it can be issued. The staff should develop a plan to complete an integrated staff guidance document for DI&C defense-in-depth and diversity assessments to maintain consistency across all reactor types. Longer term suggestions to improve assessments of defense in depth and diversity are included.

Sincerely,

Halnon, Gregory signing on behalf of Kirchner, Walter on 03/22/24

Walter L. Kirchner
Chair

REFERENCES:

1. U.S. Nuclear Regulatory Commission, "NUREG-0800, Branch Technical Position 7-19, 'Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems'," [Final Revision 9 – 202X], February 16, 2024 (ML24005A077).

2. U.S. Nuclear Regulatory Commission, "NUREG-0800, Branch Technical Position 7-19, 'Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems'," Revision 8, January 2021 (ML20339A647).

3. U.S. Nuclear Regulatory Commission, SRM-SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993 (ML003708056).

4. U.S. Nuclear Regulatory Commission, SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," September 12, 2018 (ML18179A067).

5. U.S. Nuclear Regulatory Commission, SRM-SECY-22-0076, "Staff Requirements—SECY-22-0076—Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems," May 25, 2023 (ML23145A181 and ML23145A182).

6. U.S. Nuclear Regulatory Commission, RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," Revision 0, June 2020 (ML20091L698).

7. U.S. Nuclear Regulatory Commission, RG 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Revision 3, January 2018 (ML17317A256).

8. U.S. Nuclear Regulatory Commission, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” NUREG/CR-6303, December 1994 (ML071790509).

9. U.S. Nuclear Regulatory Commission, “Design Review Guide (DRG): Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews,” February 26, 2021 (ML21011A140).

March 22, 2024

SUBJECT: FINAL DRAFT REVISION 9 OF STANDARD REVIEW PLAN BRANCH TECHNICAL POSITION 7-19, "GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON-CAUSE FAILURE DUE TO LATENT DEFECTS IN DIGITAL SAFETY SYSTEMS"

Accession No: ML24075A286 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	LBurkhart	RKrsek	SMoore	WKirchner *(GHalnon for)*
DATE	03/15/24	03/15/24	03/18/24	03/21/24	03/22/24	03/22/24

OFFICIAL RECORD COPY